

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND  
NORTHERN DIVISION

Cotton Patch CAFE, INC.

Plaintiff,

v.

MICROS SYSTEMS, INC.,

Defendant.

)  
)  
)  
)  
)  
)  
)  
)

CASE NO. MJG-09-cv-3242

**PLAINTIFF COTTON PATCH CAFE, INC.'S MEMORANDUM  
IN SUPPORT OF OPPOSITION TO DEFENDANTS' MOTION IN LIMINE  
TO LIMIT TESTIMONY OF PLAINTIFF'S EXPERT ROGER NEBEL**

---

**TABLE OF CONTENTS**

ROGER NEBEL’S EXPERIENCE AND QUALIFICATIONS ..... 2

ARGUMENT AND AUTHORITIES..... 6

    I.    Micros agrees that Nebel is qualified to provide expert testimony about  
          several technical data security and computer forensics issues in this case.....6

    II.   Nebel will not offer expert opinions concerning witness credibility, fact  
          questions within the common knowledge of the jury, or purely legal  
          questions. ....7

    III.  Nebel is qualified to offer expert opinions concerning the customs and  
          practices in the IT security and outsourcing business and communications  
          between software vendors and their customers concerning information  
          security. ....8

        A.   Nebel is qualified to testify as an expert about whether it is common for  
              merchants to outsource their IT security functions to third-party service  
              providers on a “buy-as-you-go” basis.....9

        B.   Nebel is qualified to offer expert opinions about whether it is common and  
              expected for a software vendor like Micros to promptly notify its  
              customers about security vulnerabilities and flaws in the vendor’s  
              software, and the form those notifications should take.....11

        C.   Nebel is qualified to opine on whether Cotton Patch could properly rely  
              upon Micros’ representations about the security and compliance of the  
              Micros POS system when assessing its data security needs. ....12

    IV.  Nebel’s testimony concerning the presence of malware on the Micros POS  
          system installed at the Cotton Patch Nacogdoches restaurant is directly  
          relevant to Cotton Patch’s remaining fraud by nondisclosure claim. ....13

CONCLUSION..... 13

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>CASES</b>	
<i>Belk, Inc. v. Meyer Corp., U.S.</i> , 679 F.3d 146 (4th Cir. 2012) .....	9
<i>Kopf v. Skyrn</i> , 993 F.2d 374 (4th Cir. 1993) .....	10
<i>Pulse Med. Instruments, Inc. v. Drug Impairment Detection Servs., LLC</i> , 858 F.2d 505 (D. Md. 2012) .....	11
<i>United States v. Pansier</i> , 576 F.3d 726 (7th Cir. 2009) .....	9
<i>Walters v. Prince George's Cnty.</i> , No. 8:08-CV-00711, 2013 WL 497920 (D. Md. Feb. 7, 2013) .....	12
<b>OTHER AUTHORITIES</b>	
Fed. R. Evid. 703 .....	12

**PLAINTIFF COTTON PATCH CAFE, INC.'S MEMORANDUM  
IN SUPPORT OF OPPOSITION TO DEFENDANTS' MOTION IN LIMINE  
TO LIMIT TESTIMONY OF PLAINTIFF'S EXPERT ROGER NEBEL**

In its Motion in Limine ("Motion") Micros makes straw man arguments against expert "opinions" that Nebel will not give, and that Cotton Patch never intended to offer. Nebel will not testify about the credibility of the witnesses or instruct the jury on the law of the case. Nor will Nebel opine on matters that are within the common knowledge of the jurors. Because most of the challenges raised in Micros' Motion address opinions that Nebel will not offer at trial, Micros' Motion is largely moot.

Micros does attack a handful of valid expert opinions that Nebel is fully qualified to offer at trial. Those opinions are: (1) it is common for merchants to outsource their information technology ("IT") security functions to third-party service providers, often on a "buy-as-you-go" basis; (2) it is common and expected for a software vendor like Micros to promptly notify its customers about security vulnerabilities and flaws in the vendor's software; and (3) Cotton Patch could properly rely upon Micros' representations about the security and compliance of the Micros POS system when assessing its own compliance with data security standards.

Micros attacks those opinions by attempting to arbitrarily confine Nebel's expertise to the forensic examination of computer security systems and the contents and evolution of data security standards. *See* Motion at 5, 8, 11. That ignores Nebel's broad and lengthy experience in the IT security field as a business executive who managed software security vulnerability notification programs. It also ignores Nebel's business experience working with clients who outsourced portions of their IT security function to companies where Nebel was employed. Nebel's experience is sufficiently broad to cover all of the opinions that he will offer at trial,

including testimony regarding customary practices in relationships between software vendors and their customers. Accordingly, to the extent Micros challenges expert opinions that Nebel will offer at trial, Micros' Motion should be denied.

### **ROGER NEBEL'S EXPERIENCE AND QUALIFICATIONS**

As Micros readily concedes, Roger Nebel is highly qualified to offer expert opinions about computer forensics and payment card data security standards. Nebel's qualifications are much broader, however, and include experience delivering a variety of IT security services to merchants and clients. Accordingly, Nebel is qualified to testify as an expert on customs and practices in the IT security outsourcing business and communications between software providers and their customers concerning software security issues.

Nebel has over thirty years of direct technical work, consulting, management responsibilities, and executive experience in the federal and commercial IT and information security markets. *See* Exh. 1 (Nebel Resume). He has worked with computers for most of his professional career. Nebel holds a bachelor's degree in engineering, and a master's degree in business management. *See* Exh. 2 (Nebel Dep. vol. 1) at 148:12–149:6, 158:20–159:4. He served in the United States Navy as a fire control technician on a submarine, *id.* at 150:1–152:16, and later worked as a contractor for the defense industry providing highly technical computer-related services, *id.* at 153:15–154:3, 157:4–158:19.

Nebel has worked on IT security issues since the mid-1990's when the Internet first became widely available for commercial use. In 1996, Nebel co-founded an Internet security firm called HomeCom Internet Security Services, which was later acquired by HomeCom Communications. *Id.* at 163:4–165:17. While with HomeCom, Nebel led Internet security

consulting projects for major financial institutions, including Pershing and Citibank, and conducted security audits on Internet banking websites. Exh. 4 (Nebel Dec.) ¶ 5. Nebel left HomeCom in 1999 to work for iDefense as its Chief Technology Officer from 1999 to 2001. Exh. 4 (Nebel Dec.) ¶ 6. While at iDefense, Nebel performed malware analysis and built a computer security database that tracked software vulnerabilities, patches, and malware. Exh. 2 (Nebel Dep. vol. 1) at 165:18–167:14. Nebel was part of a high-performance team that tracked software security vulnerabilities for numerous software products, and provided notification of those vulnerabilities, and patches, to clients. Exh. 4 (Nebel Dec.) ¶ 6. Nebel worked directly with software vendors to craft appropriate notice of vulnerabilities and patches to be distributed to the software users. *Id.*

In 2001, Nebel joined TruSecure as its Vice President of Services. Exh. 4 (Nebel Dec.) ¶ 7. While at TruSecure, Nebel oversaw the defined security program, which provided IT security services to over 1,000 online customers, including Internet banks, retail merchants, and payment processing services companies such as ExxonMobil Speedpass. *Id.* Nebel managed and worked with TruSecure's IT security certification product offering and TruSecure's security consulting arm. *Id.* TruSecure's product offerings on which Nebel worked included IT security outsourcing services for clients such as retail merchants. *Id.* In that role, Nebel gained direct, personal experience managing numerous IT security outsourcing relationships, and became familiar with customary practices in the IT and Internet security outsourcing industry. *Id.*

In 2005, Nebel joined FTI Consulting, where he was the national practice lead providing data security consulting services to merchants. Exh. 4 (Nebel Dec.) ¶ 8. While at FTI, Nebel worked as a Cardholder Information Security Program ("CISP") and Payment Card Industry

Data Security Standard (“PCI DSS”) certified assessor, and led teams that audited and reported on several data security breaches involving point-of-sale systems. Exh. 3 (Nebel Dep. vol. 2) at 652:20–653:2; Exh. 4 (Nebel Dec.) ¶ 8. Nebel was also certified to conduct audits of POS systems—like the Micros POS system at issue in this case—under Visa’s Payment Application Best Practices (“PABP”) and, later, under the Payment Application Data Security Standard (“PA DSS”). Exh. 4 (Nebel Dec.) ¶ 8. While at FTI, Nebel conducted a breach investigation of a restaurant chain that was using a Micros POS system. *Id.* Nebel and FTI were also engaged by Catholic Healthcare West, the largest not-for-profit hospital chain in the Southwest, to audit and assess over 200 card swipe machines and POS systems, including the Micros RES system. Exh. 2 (Nebel Dep. vol. 1) at 200:10–201:11, 203:20–204:7.

Since 2009, Nebel has served as Managing Director of Defense Group, Inc.’s cyber security business unit serving state, federal, and local government clients. Exh. 4 (Nebel Dec.) ¶ 9. Nebel also serves as Defense Group’s Chief Information Security Officer. *Id.* Nebel serves as a subject-matter expert for various government entities on Internet security, malware, hacking, and related technical issues. *Id.* In that role, Nebel researches and reports on a wide variety of IT security issues, reverse engineers malware, and tracks and alerts on emerging cyber threats and trends. *Id.*

Nebel holds several professional credentials and certifications that further qualify him to testify as an expert in this case. At present, Nebel is a Certified Information System Security Professional (“CISSP”), and a Certified Information System Auditor (“CISA”). Exh. 1 (Nebel Resume). The CISSP is conferred by the International Information Systems Security Certification Consortium to candidates who pass an examination, and must be maintained by

acquiring annual continuing professional education credits. Exh. 3 (Nebel Dep. vol. 2) at 392:6–394:15. The CISSP certification qualifies an individual to pursue certification as a Qualified Security Assessor. Exh. 4 (Nebel Dec.) ¶ 3(a). The CISA, in turn, is conferred by the Information Systems Audit and Control Association to candidates who pass an examination, and must be maintained by acquiring annual continuing professional education credits. Exh. 2 (Nebel Dep. vol. 2) at 392:6–394:15. A person holding a CISA is licensed to perform information technology governance audits, which include analysis of an organization’s IT security and controls, including its outsourcing and vendor relationships. *Id.* at 616:1–9; Exh. 4 (Nebel Dec.) ¶ 3(b).

While working at FTI from 2005 to 2009, Nebel also was a Qualified Security Assessor (“QSA”). The QSA designation is conferred on individuals who meet specific information security education requirements, have taken appropriate training from the Payment Card Industry (“PCI”) Security Standards Council, and are employed by a designated Qualified Security Company. Exh. 4 (Nebel Dec.) ¶ 4. The QSA designation qualifies an individual to perform PCI consulting and compliance auditing relating to the protection of credit card data. *Id.* A QSA performs assessments of merchants to determine if they meet compliance requirements like Visa’s Cardholder Information Security Program (“CISP”) or the Payment Card Industry Data Security Standard (“PCI DSS”). Exh. 2 (Nebel Dep. vol. 1) at 219:4–14. Nebel also held certifications as a Qualified Payment Application Security Professional (“QPASP”) and a Qualified Data Security Professional (“QDSP”), which qualified him to perform evaluations of POS systems for compliance with Visa and PCI standards pertaining to payment applications. Exh. 4 (Nebel Dec.) ¶ 4.



Nebel has also taught courses on data security, first at the University of Virginia, and later at Georgetown University in its Master of Professional Studies in Technology Management program. Exh. 1 (Nebel Resume); Exh. 2 (Nebel Dep. vol. 1) at 181:9–185:2. At Georgetown, Nebel presently is the lead instructor for four technology courses: IT Security Compliance/Forensics, Information Assurance and Risk Assessment, Cryptography and Network Security, and Threats/Vulnerabilities. Exh. 2 (Nebel Dep. vol. 1) at 184:3–185:2.

Nebel's long experience in the IT security industry qualifies him to opine as an expert on issues that go far beyond the technical details of a forensic examination or the content of data security standards. Nebel is qualified to testify as an expert about customs and practices in the IT security industry, including communications between software vendors and their consumers concerning the security of their software products.

### **ARGUMENT AND AUTHORITIES**

#### **I. Micros agrees that Nebel is qualified to provide expert testimony about several technical data security and computer forensics issues in this case.**

Micros agrees that Nebel is qualified to give expert testimony in several areas. These include “the forensic examination of computer systems to determine whether there has been a security breach and to try to determine how it occurred, security of computer systems and the contents of the Payment Card Industry Data Security Standards (‘PCI-DSS’) and its antecedents.” Motion at 1. Micros also agrees that Nebel's experience qualifies him to offer expert opinions about “his examination of the hard-drive of the POS system that was in place at the Cotton Patch Nacogdoches restaurant at the time of the intrusion, and to give opinions about PCI-DSS.” *Id.* at 5.

Nebel will offer expert opinion testimony concerning topics in these areas, including, *inter alia*, whether and how the Micros POS server installed at the Cotton Patch Nacogdoches restaurant (“Nacogdoches POS system”) complied (and facilitated Cotton Patch’s compliance) with relevant data security standards; the presence of unencrypted full track data on the Nacogdoches POS system; the content, application, and purpose of accepted data security standards; the general operation and structure of the payment card industry; and Nebel’s forensic examination of the Nacogdoches POS system hard drive. Because Micros agrees that Nebel is qualified to testify about those topics, and because that testimony is relevant to the issues in this case, Nebel’s expert opinions in these areas should be admitted at trial.

---

**II. Nebel will not offer expert opinions concerning witness credibility, fact questions within the common knowledge of the jury, or purely legal questions.**

Most of Micros’ Motion is devoted to attacking “opinions” that Nebel will not give, and that Cotton Patch never intended to offer, at trial. Specifically, Nebel will not offer expert testimony concerning the following issues:

- Whether Micros actually made representations to Cotton Patch concerning (a) the Nacogdoches POS system, (b) Micros’ role in maintaining the security of Cotton Patch’s systems, and (c) the compliance of those systems with prevailing data security standards. *See* Motion at 7 (second, third, and fourth bullet points), 8 (first, second, and third bullet points), 15 (second bullet point).
- Whether Micros actually failed to disclose facts about the non-compliance of Micros POS systems with prevailing data security standards. *See* Motion at 7 (fourth bullet point), 15 (third bullet point); 18 (third, fifth, and sixth bullet points).
- Whether Cotton Patch subjectively relied upon representations and non-disclosures by Micros concerning (a) the Nacogdoches POS system, (b) Micros’ role in maintaining the security of Cotton Patch’s systems, and (c) the compliance of those systems with prevailing data security standards. *See* Motion at 7 (second, third, and fourth bullet points); 8 (second and fourth bullet points), 9 (second

bullet point), 12 (first bullet point); 15 (first, second, fourth, and sixth bullet points); 16 (first bullet point).

- Whether Cotton Patch is in the IT provision business, and whether Cotton Patch actually relied upon Micros to fill the role of IT provider. *See* Motion at 9 (first bullet point).
- Whether Micros actually directed Alan Mann to “stay out” of the Nacogdoches POS system. *See* Motion at 17 (first bullet point).
- Whether Cotton Patch actually received notices from Micros concerning compliance with data security standards, and what Cotton Patch would have done in response to those notices. *See* Motion at 14 (text), 18 (third, fifth, and sixth bullet points), 19 (first bullet point).
- Whether Micros was actually aware of security deficiencies and vulnerabilities in its POS products, including the Nacogdoches POS system. *See* Motion at 15 (third bullet point), 17 (first bullet point), 18 (second and fifth bullet points), 19 (first bullet point).

In addition, Nebel is not going to offer expert opinions about purely legal questions, such as the legal interpretation of contracts between Cotton Patch and Micros.

Contrary to Micros’ argument, Nebel will not offer expert opinions that invade the province of either the Court or the jury. Instead, Nebel will offer expert opinions based on his extensive experience and qualifications on subjects that are outside the common understanding of the jury, and that are helpful and relevant to the resolution of this case. Micros’ straw man arguments provide no basis to limit Nebel’s testimony regarding his actual expert opinions.

**III. Nebel is qualified to offer expert opinions concerning the customs and practices in the IT security and outsourcing business and communications between software vendors and their customers concerning information security.**

Nebel is qualified to offer expert testimony about all of the following issues raised in Micros’ motion: (1) whether it is common for merchants to outsource their information technology and data security functions to third-party service providers, often on a “buy-as-you-go” basis; (2) whether it is common and expected for a software vendor like Micros to promptly

notify its customers about security vulnerabilities and flaws in the vendor's software and the form of that notice; and (3) whether Cotton Patch could properly rely upon Micros' representations about the security and compliance of the Micros POS system when assessing its data security needs.

Nebel is qualified to opine on those issues based on his broad and lengthy experience in the information technology security business. *See Belk, Inc. v. Meyer Corp., U.S.*, 679 F.3d 146, 162 (4th Cir. 2012) (stating that a court must “consider the proposed expert's full range of experience and training” when deciding whether an expert is qualified to render an expert opinion (quoting *United States v. Pansier*, 576 F.3d 726, 737 (7th Cir. 2009))). Accordingly, he should not be prevented from offering expert opinions on those issues at trial.

**A. Nebel is qualified to testify as an expert about whether it is common for merchants to outsource their IT security functions to third-party service providers on a “buy-as-you-go” basis.**

Nebel is qualified based on his experience in the IT security and outsourcing business to offer expert opinion testimony about whether merchants commonly outsource their IT security functions to third-party service providers on a “buy-as-you-go” basis. Nebel worked for IT service providers from 1996 to 2005. Exh. 2 (Nebel Dep. vol. 1) at 163:4–167:14; Exh. 4 (Nebel Dec.) ¶¶ 5–7. During that time, he managed relationships between providers of outsourced IT security services and their clients. Exh. 4 (Nebel Dec.) ¶¶ 6–7. Based on that experience, Nebel is well qualified to testify about whether it is common for retail merchants to outsource much or all of their IT security function to a third-party vendor, and the typical nature of those relationships. In addition, that same experience, as well as Nebel's experience as a QSA, qualifies Nebel to opine on whether Cotton Patch is a relatively sophisticated merchant with

respect to IT security issues compared to other merchants that outsource their IT security function.

Nebel's qualifications are not diminished by the fact that he has not worked for a POS vendor like Micros, or spent significant time working in a restaurant. Micros argues that Nebel cannot opine on the "post sale duties" that payment card vendors owe to restaurant customers because he was not worked in either industry. *See* Motion at 10–11. That argument mischaracterizes Nebel's testimony and draws the relevant range of experience far too narrowly. Cotton Patch alleges that Micros made representations that the Nacogdoches POS system was compliant with applicable data security standards, and that Cotton Patch relied upon Micros to maintain its POS systems in a secure and complaint manner. Nebel is qualified to opine as to whether the relationship between Cotton Patch, as a consumer of software and IT services, and Micros, as a provider of software and IT services, was customary and typical of an IT outsourcing relationship. That testimony, in turn, is relevant, *inter alia*, to whether Cotton Patch reasonably relied upon Micros' misrepresentations concerning the compliance and security of Micros products, including the Nacogdoches POS system.<sup>1</sup>

---

<sup>1</sup> Micros also argues that Nebel's testimony should be excluded because he was not aware of specific standards or data on the frequency and type of outsourcing relationships. *See* Motion at 11–12. Whether Nebel reviewed specific "standards or data" on outsourcing is not a prerequisite to the admissibility of his testimony. Nebel based his opinion on his experience in the industry and his conversations with a professional colleague who studies the outsourcing and insourcing markets. *See* Exh. 2 (Nebel Dep. vol. 1) at 327:2–331:18; *see also* Exh. 4 (Nebel Dec.) ¶¶ 6–7. Nebel's experience and investigation is more than adequate to support Nebel's opinion that IT security outsourcing relationships are "common." *See Kopf v. Skyrms*, 993 F.2d 374, 377 (4th Cir. 1993) (finding that a person "may qualify to render expert testimony in any one of the five ways listed [in Rule 702]: knowledge, skill, experience, training, or education").

**B. Nebel is qualified to offer expert opinions about whether it is common and expected for a software vendor like Micros to promptly notify its customers about security vulnerabilities and flaws in the vendor's software, and the form those notifications should take.**

Nebel is qualified to offer expert opinions about whether a software vendor like Micros would typically notify its customers about security vulnerabilities and flaws in the vendor's software, and the form that notification should take. Nebel worked for three companies—HomeCom, iDefense, and TruSecure—that provided IT consulting and security services to a variety of clients, including retail merchants. Exh. 2 (Nebel Dep. vol. 1) at 163:4–167:14; Exh. 4 (Nebel Dec.) ¶¶ 5–7. At two of those companies, Nebel worked directly with software vendors and merchants to facilitate notification of security vulnerabilities and threats associated with commercial software applications. Exh. 2 (Nebel Dep. vol. 1) at 166:20–167:14; Exh. 4 (Nebel Dec.) ¶¶ 6–7. That experience qualifies Nebel to testify about the customary practices of software vendors to notify their customers about security vulnerabilities in their software offerings, and the way in which that notification should be provided in order to be effective. That testimony is directly relevant to Cotton Patch's fraud by nondisclosure claim.

Micro's argument that Nebel lacks such qualifications because he has not worked in the POS or restaurant industries ignores Nebel's highly relevant experience in the data security business and, in particular, his experience facilitating the communication of such notification from vendors to merchants. Nebel is not disqualified from offering these opinions merely because he has not worked for a POS software vendor or run a restaurant. His testimony concerns the broader subject of communication between software vendors and their customers—a field in which Nebel has direct and relevant experience. *See Pulse Med. Instruments, Inc. v. Drug Impairment Detection Servs., LLC*, 858 F.2d 505, 511 (D. Md. 2012) (noting that “the

requirement that the area of an expert's competence match the subject matter of his testimony 'does not mean that an opinion on a given issue can only be given by an expert in a single, specific discipline'" (quoting 29 Charles Alan Wright & Victor J. Gold, Federal Practice and Procedure § 6265 (2011)); *Walters v. Prince George's Cnty.*, No. 8:08-CV-00711, 2013 WL 497920, at \*5 (D. Md. Feb. 7, 2013) (finding that "[w]hile an expert's qualification in one area does not automatically qualify him to testify in a related area, the expert's specialized knowledge and experience and the issues before the court need not be exact") (denying motion to limit expert testimony).<sup>2</sup>

**C. Nebel is qualified to opine on whether Cotton Patch could properly rely upon Micros' representations about the security and compliance of the Micros POS system when assessing its data security needs.**

Nebel is qualified to offer expert opinion testimony about whether Cotton Patch was justified in relying on representations by Micros concerning the security and compliance of Micros POS systems. As a CISA and former QSA, Nebel is qualified and credentialed to

---

<sup>2</sup> Micros argues that Nebel is not qualified to testify that it is common in the POS software industry for vendors to offer free, automatic software upgrades to their customers. Motion at 12–13. Nebel does not advance that position, and will not offer that testimony at trial. Instead, Nebel will testify about the customary practice of software vendors like Micros to notify their customers of security vulnerabilities and flaws in their software products. Micros also argues that Nebel is not qualified to testify that use of common and default userids and passwords was an "endemic issue" to Micros because Nebel did not perform a breach investigation of a Micros product in which common and default userids and passwords were at issue. *Id.* at 13–14. Regardless of whether Nebel personally investigated a breach involving common and default userids and passwords, he is qualified to testify about whether use of such userids and passwords violates relevant data security standards, and whether such use presents an information security risk. Moreover, Nebel is entitled to apply his expertise to evidence presented in this case of other breaches of Micros systems to determine whether Micros systems exhibited patterns of security vulnerability, including use of common and default userids and passwords. *See* Fed. R. Evid. 703 (stating that an expert may base his opinion on facts or data in the case that the has been made aware of or personally observed).

conduct security audits of merchants like Cotton Patch. As part of that audit process, a CISA must determine whether a merchant has appropriately relied upon a third party, such as a software vendor or security outsourcing firm, to ensure certain aspects of that merchant's data security. Exh. 3 (Nebel Dep. vol. 2) at 616:1-9; Exh. 4 (Nebel Dec.) ¶ 3(b). Thus, Nebel is qualified to testify that, to the extent Micros made representations concerning the security and compliance of the Micros POS system, Cotton Patch was entitled to rely on those representations as part of its data security efforts. These opinions, in turn, are directly relevant to whether Cotton Patch's reliance on Micros' representations was reasonable and appropriate in light of well-accepted auditing standards.

---

**IV. Nebel's testimony concerning the presence of malware on the Micros POS system installed at the Cotton Patch Nacogdoches restaurant is directly relevant to Cotton Patch's remaining fraud by nondisclosure claim.**

Nebel's expert opinions concerning the presence of malware on the Nacogdoches POS system before it was installed by Micros is directly relevant to Cotton Patch's fraud by nondisclosure claim that remains pending in this case. *See* Memorandum and Order Regarding Reconsidered Motions, at 19-22 (ECF 151). Micros does not challenge Nebel's qualifications to give this opinion. Accordingly, Nebel's opinion regarding the malware on the Nacogdoches POS system is relevant and admissible with respect to Cotton Patch's fraud by nondisclosure claim. Micros' argument that this testimony is no longer relevant is patently inaccurate. *See* Motion at 20.

**CONCLUSION**

Micros asks this Court to exclude expert opinions about factual and legal issues that Nebel will not give at trial, and that Cotton Patch never intended to offer. As for Nebel's expert



opinions that Micros does properly challenge, Nebel is well qualified to offer those opinions based on his extensive background providing information technology and data security services. To the extent Micros challenges Nebel's qualifications to offer expert opinions that Cotton Patch intends to offer at trial, Micros' motion should be denied.

Dated: May 30, 2013

Respectfully submitted,

/s/ Craig D. Roswell

Craig D. Roswell

Federal Bar No. 433406

**Niles, Barton & Wilmer, LLP**

111 South Calvert Street, Suite 1400

Baltimore, Maryland 21202

[cdroswell@nilesbarton.com](mailto:cdroswell@nilesbarton.com)

Telephone: 410.783.6341

Facsimile: 410.783.6486

Robert N. LeMay

*Admitted Pro Hac Vice*

**Kane Russell Coleman & Logan, P.C.**

1601 Elm Street, Suite 3700

Dallas, Texas 75201

[rlemay@krcl.com](mailto:rlemay@krcl.com)

Telephone: 214.777.4200

Facsimile: 214.777.4299

AND

Ryan L. Bangert

*Admitted Pro Hac Vice*

**Baker Botts L.L.P.**

2001 Ross Avenue, Suite 600

Dallas, Texas 75201

[ryan.bangert@bakerbotts.com](mailto:ryan.bangert@bakerbotts.com)

Telephone: 214.953.6621

Facsimile: 214.661.4621

**ATTORNEYS FOR PLAINTIFF  
COTTON PATCH CAFÉ, INC.**

**CERTIFICATE OF SERVICE**

I HEREBY CERTIFY that on this 30th day of May 2013, a true and correct copy of the foregoing Memorandum in Support of Opposition to Defendant's Motion in Limine to Limit the Testimony of Plaintiff's Expert Roger Nebel was served via the Court's ECF system on the following:

Steven A. Allen  
Pessin Katz Law, P.A.  
901 Dulaney Valley Road, Suite 400  
Towson, Maryland 21204  
*Attorney for the Defendant*

/s/ Craig D. Roswell  
Craig D. Roswell  
**Niles, Barton & Wilmer, LLP**  
111 South Calvert Street, Suite 1400  
Baltimore, Maryland 21202